H.C. Starck setzt auf eine umfassende und integrierte Security Strategie mit McAfee.

Dank seiner einzigartigen Kompetenz für hochschmelzende Metalle und technische Keramiken ist H.C. Starck heute mehr denn je Partner für innovative Produkte mit hoher Wertschöpfung

» Eine gute Betreuung und Unterstützung vor, während und nach dem Projekt ist entscheidend gewesen für den Erfolg. Durch die immer komplexeren Bedrohungen ist ein guter Partner eine wichtige Stütze.«

Alwin Großekatthöfer
Director Corporate Infrastructur
H.C. Starck GmbH

H.C. Starck ist ein internationaler Konzern mit mehr als 2.900 Mitarbeitern an 12 Produktionsstandorten in Europa, Nordamerika und Asien. Das Unternehmen produziert hochschmelzende Metalle (Refraktärmetalle) und technische Keramiken sowohl in Pulverform oder als kundenspezifisches Bauteil. Mit den nach ISO 9001 zertifizierten Standorten und den starken internationalen Verflechtungen ist eine enge datenmäßige Vernetzung erforderlich - trotz all den damit verbundenen Risiken.

Auf der Suche nach einer umfassenden Security Lösung, die das Unternehmen bei ihrem internationalen Geschäft zuverlässig auf allen Ebenen schützt, kam die IT-Abteilung ins Gespräch mit der Firma Bücker EDV.
Gemeinsam wurden die Anforderungen und Herausforderungen analysiert, die eine komplexe Unternehmensstruktur wie die von H.C. Starck darstellt. Diese Untersuchungen ergaben, dass nur McAfee mit seinem umfangreichen Security Portfolio und der zentralen Managementkonsole ePolicy Orchestrator der Aufgabe gewachsen ist.
Neben dem Virenschutz, der bereits für sich genommen eine komplexe Aufgabenstellung ergibt, sollten auch die Standorte und Subnetze untereinander abgesichert werden. Dabei war wichtig, dass Bedrohungen und Angriffe noch effektiver am Gateway abgewehrt werden können und falls sie durch andere Wege ins Netzwerk gelangen, niemals das ganze Netzwerk erreichen.

McAfee bietet dafür mit der Kombination der Virenschutz- und der netzwerkbasierten Intrusion Prevention Systeme einen einzigartigen Ansatz die Anforderungen effektiv zu erfüllen und den Sicherheitslevel auf höchstes Niveau zu heben.

Anforderungen:
Für das neue Virenschutzkonzept waren vor allem folgende Kriterien elementar:

- Einheitliches Enterprise Management für alle Produkte, die auf den Endgeräten installiert werden (AntiVirus, Host Intrusion Prevention, etc.)
- Erkennen und entfernen des bisher eingesetzten Produktes
- Umfangreiches Reporting (auf Abruf und per Zeitplanung)
- Rollenbasierte Multiuser Management Konsole, Browser basierend
- Langfristige Speicherung der Ereignisdaten in einer zentralen Datenbank
- Umfangreiche technische Unterstützung in allen Phasen durch einen kompetenten Partner (Produktauswahl, Planung, Einführung)

Die ergänzende Netzwerksicherheit sollte zudem vor allem:

- Angriffe und Schädlinge in Echtzeit abwehren, inklusive Zero-Day-, Denial-of-Service- und Distributed-Denial-of-Service-Angriffen
- Angriffe über erlaubte Verbindungen in erlaubten Protokollen unterbinden
- Anomalien im Netzwerkverkehr aufzeigen
- Richtlinienbasiert, unterschiedlich mit Angriffen auf verschiedene Rechner verfahren
- Möglichst nahtlos in die vorhandene Infrastruktur der IT-Security integrierbar sein
- Möglichst zentral verwaltet werden können

R. BÜCKER
EDV-Beratung Datentechnik GmbH

H.C.Starck

» Die Integrationsmöglichkeiten der McAfee Virenschutz- und Netzwerk Intrusion Prevention-Lösungen machen es uns überhaupt erst möglich, die Vorteile dieser Lösungen zu nutzen.«

Alwin Großekatthöfer
Director Corporate Infrastructur
H.C. Starck GmbH

McAfee

Testphase:
Die von der R. Bücker EDV vorgeschlagenen Lösungen, der Virenschutz und die Network Security Platform von McAfee, wurden in einem WebCast vorgestellt und dabei live im Einsatz gezeigt, um der IT-Abteilung einen ersten Eindruck der Möglichkeiten zu verschaffen.

Da die bereits beschriebenen Anforderungen in vollem Umfang und zusätzlich aus einer Hand erfüllt werden konnten, wurde im nächsten Schritt die Testphase geplant. Dabei sollten sowohl Virenschutz, als auch Netzwerk IPS in der LiveUmgebung von H.C. Starck, gemeinsam mit den System Ingenieuren der Firma Bücker evaluiert werden, um realistische Bedingungen zu schaffen.

Die Hardware Appliance von McAfee wurde vorbereitet und dann gemeinsam mit den Administratoren der H.C. Stark in das Netzwerk integriert. Die Transparenz des Systems sorgte dabei dafür, dass keine Anpassungen in der Infrastruktur notwendig waren.
Die zentrale Managementkonsole ePO wurde parallel zu der Konsole des bisherigen Virenschutzherstellers aufgesetzt. Nach der Grundkonfiguration, Erstellung der ersten Richtlinien und einer Testgruppe, konnte die neue Software direkt auf die ersten Systeme verteilt werden. Die Software des Drittanbieters wurde dabei automatisch erkannt und deinstalliert. Die weitere Testphase verlief so störungsfrei, dass das Virenschutz System direkt übernommen werden konnte. Der unternehmensweite RollOut und langfristige Einsatz war damit ohne eine erneute Installation möglich.

Ergebnis:
Nach den erfolgreichen Tests fiel die Entscheidung für die McAfee Lösungen. Dabei waren nicht nur die Tests, sondern auch weitere Faktoren ausschlaggebend:

- Das zentrale Management ePO erfüllt alle Anforderungen und bietet dazu eine hohe Investitionssicherheit, da auch bei neuen Herausforderungen, zusätzliche Sicherheitskomponenten integriert werden können.
- In den Tests der unabhängigen NSS Group hat das McAfee IPS von allen bisher getesteten Lösungen die höchste Genauigkeit und den höchsten Durchsatz aufgewiesen.
- Nicht nur Bedrohungen werden erkannt und abgewehrt, sondern auch eine unerwünschte Nutzung des Netzes, bezogen auf Unternehmensrichtlinien (z. B. File Sharing), kann unterbunden werden, ohne dass sicherheitsrelevante Aspekte im Vordergrund stehen

Umsetzung:
Die Implementierung der ersten beiden IPS Appliances erfolgte zweistufig. Der Einbau der Appliances und die Verkabelung wurden komplett von der H. C. Starck durchgeführt. Beim ersten Termin wurden nach der eigentlichen Installation Grundeinstellungen vorgenommen und die zuständigen Administratoren durch die Spezialisten der Firma Bücker EDV geschult.
Schon direkt nach der Installation zeigte sich, dass das System relativ schnell eingesetzt werden kann, um einen „vernünftigen" Grundschutz zu gewährleisten. Die von McAfee mitgegebenen Richtlinien sind hier eine große Hilfe.

Die Integration in den ePolicy Orchestrator wurde durchgeführt, um die Vorteile des Datenaustauschs nutzen zu können. Das bedeutet, dass der ePO in Form von Dashboards Informationen über den Systemzustand des IPS zeigt. Umgekehrt werden Informationen über einzelne Rechner bzgl. des AV-Status bzw. des aktuellen Schutzzustandes und Host Intrusion Prevention-Meldungen an das Netzwerk-IPS übermittelt.

Weiterer Betrieb:
Einige Wochen später wurden in einem Folgetermin erste Erfahrungen ausgewertet, Fragen geklärt und weitere Feineinstellungen vorgenommen.
Gerade der Datenaustausch unter den Systemen bewies sich hier als besonders wertvoll. Alarmmeldungen, die in der Regel für die Abschreckung vor dem Einsatz einer solchen Lösung sorgen, können so automatisch priorisiert werden. Die Administratoren müssen sich dadurch nur noch um Meldungen mit hoher Priorität kümmern.

R.Bücker EDV Beratung Datentechnik GmbH
Nordhemmer Str. 95/97
32479 Hille
Tel: 05703-930-0
Fax: 05703-930-390
info@buecker-edv.de
www.buecker-edv.de

» Mit dem ePolicy Orchestrator haben wir ein Werkzeug erhalten, das uns in die Lage versetzt, einen zentralen Überblick der Bedrohungslage zu bekommen und falls nötig, effiziente Maßnahmen einzuleiten.«

Alwin Großekatthöfer
Director Corporate Infrastructur
H.C. Starck GmbH

Andere Meldungen dienen lediglich noch der Information – „Auch ohne das IPS System, wäre der Angriff auf dem Endgerät durch die bestehenden Schutzsysteme nicht erfolgreich gewesen."

Darüber hinaus zeigte sich, dass das System - über das Blocken hinaus - wertvolle Informationen über möglicherweise sicherheitsrelevante Vorkommnisse in den beteiligten Subnetzen liefert. So wird auch eine Grundlage zur Anpassung eventuell kritischer Konfigurationen eigener Systeme geboten. Damit wird nicht nur erreicht, dass die zu schützenden Subnetze nicht mehr von potentiellen Angreifern erreicht werden, sondern auch die Voraussetzungen geschaffen, dass die Rechner in diesen Subnetzen sicherheitstechnisch optimal konfiguriert werden können.

Wertvolle Informationen liefert hier auch wieder der angebundene ePO. Nach den ersten Erfahrungen am Standort Goslar wurden mittlerweile zwei weitere Maschinen angeschafft, die in München im HA-Cluster laufen.

Wegen der intuitiven Bedienbarkeit der Benutzeroberfläche konnten die Administratoren diese Appliances selbständig in Betrieb nehmen und in das vorhandene System integrieren.

Das Ergebnis des Gesamtprojektes ist eine neue und in alle Richtungen wirksame Security Strategie der H.C. Starck Gruppe.

McAfee,
eine hundertprozentige Tochtergesellschaft der Intel Corporation, ist der weltgrößte dedizierte Spezialist für IT-Sicherheit. Das Unternehmen mit Hauptsitz im kalifornischen Santa Clara hat sich der Beantwortung anspruchsvollster Sicherheitsherausforderungen verschrieben. Seinen Kunden liefert McAfee präventive, praxiserprobte Lösungen und Dienstleistungen, die Computer und ITK-Netze auf der ganzen Welt vor Angriffen schützen und es Anwendern ermöglichen, gefahrlos Verbindung mit dem Internet aufzunehmen und sich im World Wide Web zu bewegen. Unterstützt von einer preisgekrönten Forschungsabteilung entwickelt McAfee innovative Produkte, die Privatnutzern, Firmen und Behörden helfen, ihre Daten zu schützen, einschlägige Gesetze einzuhalten, Störungen zu verhindern, Schwachstellen zu ermitteln und die Sicherheit ihrer Systeme laufend zu überwachen und zu verbessern.
McAfee Labs, das weltweit anerkannte Forschungsteam aus mehr als 350 Forschern auf fünf Kontinenten, fungiert als dynamischer Informationsdienst und prognostiziert und identifiziert aufkommende Bedrohungen in aller Welt.
Weitere Informationen über McAfee finden Sie unter www.mcafee.com/de.

Die R. Bücker EDV-Beratung
ist ein international tätiges Unternehmen mit Schwerpunkten im Bereich der Datensicherheit, des Datenschutzes, der Netzwerktechnologie und einem Team von 30 Mitarbeitern. Unternehmen in allen Größenordnungen und allen Branchen vertrauen auf die Kompetenz, Zuverlässigkeit, Flexibilität und Erfahrung aus 25 Jahren Sicherheitsberatung.

Einige der Kernkompetenzen mit langjährigem, starkem Knowhow sind die Computervirenabwehr, das AV-Management und generelle IT-Sicherheit. Beratung und Konzeption zielen darauf ab, eine maßgeschneiderte Lösung zu gestalten, die jederzeit erweiterbar ist und dynamisch mit den Kunden und ihren Anforderungen mitwächst.
Neben AntiViren Lösungen betreut die R. Bücker EDV Kunden in den Bereichen Content Security, Verschlüsselung, Data Loss Prevention, Intrusion Prevention, Schwachstellen-, Patch- und Risikomanagement, NetworkAccessControl und Notfallmanagement. Zu Ihren langjährigen Kunden zählen namhafte Firmen wie z. B. TU Ilmenau, ITSC GmbH oder die Vivantes Kliniken in Berlin.